

WHAT IS CLAIMED IS:

1 1. A method for re-booting an operating system software in a data processing
2 system, comprising the steps of:

3 determining whether a buffer contains a message indicating that a BIOS image
4 for the data processing system was previously updated;

5 performing a signature verification on a remainder of the BIOS image; and

6 proceeding with re-boot of the operating system software if the signature
7 verification correctly verifies the remainder of the BIOS image.

1 2. The method as recited in claim 1, further comprising the step of:

2 not proceeding with the re-boot of the operating system software if the signature
3 verification does not correctly verify the remainder of the BIOS image.

1 3. The method as recited in claim 2, further comprising the steps of:

2 performing an update to the BIOS image previous to the determining step; and

3 storing the message into the buffer responsive to the step of performing the
4 update to the BIOS image.

1 4. A data processing system comprising:
2 means for performing an update to the BIOS image;
3 means for storing a message into a memory location wherein the message
4 indicates that the BIOS image has been updated;
5 during a subsequent re-boot of the data processing system, means for determining
6 an existence of the message;
7 responsive to a determination that the message is stored in the memory location,
8 means for performing a signature verification on a remainder of the BIOS image; and
9 means for proceeding with the re-boot of the data processing system if the
10 signature verification correctly verifies the remainder of the BIOS image.

1 5. The system as recited in claim 4, further comprising:
2 means for not proceeding with the re-boot of the data processing system if the
3 signature verification does not correctly verify the remainder of the BIOS image.

1 6. A computer program product adaptable for storage on a computer readable
2 medium and operable for re-booting an operating system software in a data processing
3 system, comprising the program steps of:
4 determining whether a buffer in the data processing system contains a message
5 indicating that a BIOS image for the data processing system was previously updated;
6 responsive to a determination that the buffer contains the message indicating that
7 the BIOS image for the data processing system was previously updated, performing a
8 signature verification on a remainder of the BIOS image; and
9 proceeding with re-boot of the operating system software if the signature
10 verification correctly verifies the remainder of the BIOS image.

1 7. The computer program product as recited in claim 6, further comprising the
2 program step of:

3 not proceeding with the re-boot of the operating system software if the signature
4 verification does not correctly verify the remainder of the BIOS image.

1 8. The computer program product as recited in claim 7, further comprising the
2 program steps of:

3 performing an update to the BIOS image previous to the determining step; and
4 storing the message into the buffer responsive to the step of performing the
5 update to the BIOS image.